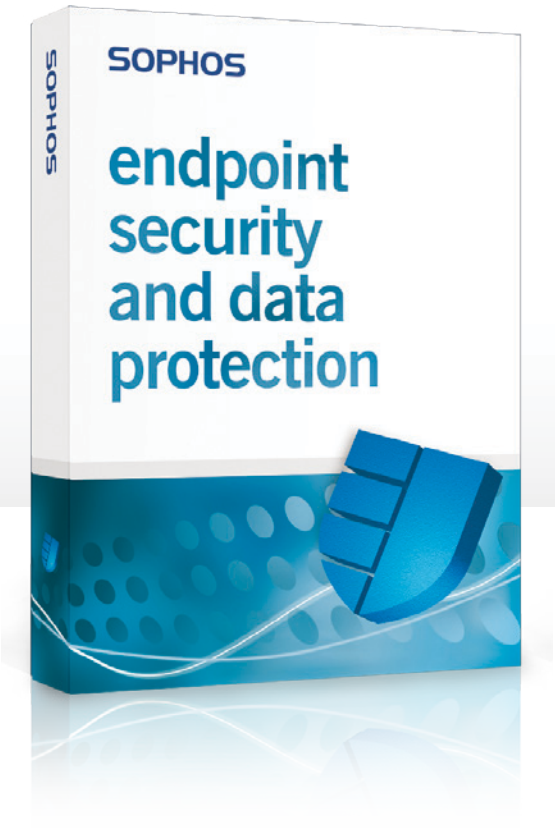
Sophos Endpoint Security and Data Protection: Reviewer's guide



SOPHOS

WELCOME

Welcome to this reviewer's guide for Sophos Endpoint Security and Data Protection – Sophos's fully integrated, scalable endpoint security solution. This document introduces the key software elements of Sophos Endpoint Security and Data Protection: management console, anti-virus, client firewall, data control, device control, application control, encryption and network access control.

The guide provides an overview of the powerful features of Sophos Endpoint Security and Data Protection. After reading it, you will have a deeper understanding of how Sophos Endpoint Security and Data Protection provides organizations with the most cost-effective and reliable protection available against known and unknown threats to computer security and how it protects your organization against data loss. It allows you to focus on other important non-security related tasks, enabling better business continuity and system efficiency.

For information on pricing and how to buy Sophos Endpoint Security and Data Protection, please contact your local Sophos representative. To find out who serves your area, please visit:

www.sophos.com/companyinfo/contacting

If you would like to request an evaluation, please go to:

www.sophos.com/products/enterprise/free-trials/

If you would like to read the installation documentation, please go to:

www.sophos.com/support/docs/

CONTENTS

1 COMPLETE PROTECTION FOR THE ENDPOINT 4
Overview of Sophos Endpoint Security and Data Protection

2 SINGLE, CENTRAL AUTOMATED CONSOLE 7
Overview of Sophos Enterprise Console

3 PROTECTING WINDOWS COMPUTERS 17
Overview of Sophos Endpoint Security and Control, Sophos Client Firewall, Sophos NAC and SafeGuard Disk Encryption

4 PROTECTING NON-WINDOWS COMPUTERS 24
Overview of Sophos Anti-Virus on Mac OS X, Linux and UNIX

APPENDICES

I EVALUATING ENDPOINT SECURITY AND DATA PROTECTION 28
Suggested test network

II THE EICAR TEST "VIRUS" 31

III OTHER SOPHOS PRODUCTS AND SERVICES 32

SOPHOS ENDPOINT SECURITY AND DATA PROTECTION

1 COMPLETE PROTECTION FOR THE ENDPOINT

OVERVIEW OF ENDPOINT SECURITY AND DATA PROTECTION

Sophos simplifies the task of securing your desktops, laptops, mobile devices, and file servers against known and unknown threats, as well as protecting your organization against accidental data loss.

Complete protection

Sophos's unified single anti-virus agent removes the need for multiple point products to stop different threats. In a single scan you can protect your organization from viruses, spyware, adware, rootkits, and potentially unwanted applications (PUAs). Simultaneously, you can control the installation and use of unauthorized software such as VoIP, Instant Messaging and peer-to-peer file sharing (P2P), control the use of removable storage devices and wireless network protocols, and monitor the transfer of sensitive information. You can also protect your data against loss with full disk encryption for your computers and encryption of information on removable storage devices as well as for secure data exchange with third parties.

Simplified, automated console

Sophos's automated console, Enterprise Console, provides a single point from which to deploy, update and report on endpoint protection across your entire estate. One console can manage tens of thousands of Windows, Mac, Linux and UNIX computers. Simplifying and automating protection drives down your costs, ensures fewer clicks per task and gives you better visibility of your entire network. In addition, role-based administration allows you to share tasks with other users to reduce your workload, whilst retaining overall control of the security policies across your entire estate.

One solution for all your platforms

When you buy an Endpoint Security and Data Protection license you get access to software that protects over 25 platforms – the widest range of any vendor – covering Windows, Mac OS X, Linux, UNIX, NetWare, NetApp Storage Systems, and Windows Mobile.

Comprehensive data protection

The combination of a number of different technologies ensures that your data is protected against accidental loss. DLP content scanning integrated into the single endpoint agent monitors for sensitive data being transferred to removable storage devices and internet-enabled applications such as email, web browsers and even Instant Messaging. Granular control of removable storage devices enables you to allow the use of specific devices, enforce the use of encrypted devices or simply allow read only access. And full disk encryption secures your data on mobile computers preventing information from getting into the wrong hands if laptops are lost.

Integrated expertise

Malware, spam, and web expertise in SophosLabs™ ensures you get the fastest and best protection. Unique technologies, such as Behavioral Genotype® Protection, combined with rapid signature updates that are small in size, stop new and unknown malware and ensure Sophos regularly beats Symantec and McAfee in independent tests.

Endpoint compliance

Sophos Endpoint Security and Data Protection ensures endpoint compliance by using Sophos NAC to assess and control all endpoint computers. Sophos NAC checks if anti-virus and other security applications are active and up to date, and whether operating systems updating patches. This reduces the risk of malware infection by quarantining and fixing vulnerable computers before access to the network is granted. Sophos NAC continues to protect throughout the user's session with periodic assessment checks.

Reasons	Benefits of Sophos
Trusted vendor	With over 20 years' experience protecting businesses from known and unknown threats, we respond rapidly to emerging threats, no matter how complex they are.
Simpler, smarter approach	Sophos Enterprise Console ensures cost-effective, centralized, intuitive management across multiple platforms, providing unrivalled visibility and control over your entire network.
Rapid response	SophosLabs keeps a round-the-clock watch on new threats, with experts analyzing new malware across every time zone and delivering the fastest, smallest updates.
Outstanding support	Technical support is delivered by a global team of Sophos experts 24x7x365, offering practical and detailed experience, which has resulted in the highest levels of customer satisfaction levels in the industry.
Simple licensing	A single subscription based licence delivers constant, automatic updates and upgrades for all new releases, as well as 24/7 in-house technical support with no hidden costs.
Pure business focus	Sophos sells only to corporate customers, ensuring all engineering, support, and research is focused on the needs of organizations, and is not diluted by the need to support consumers.

Table 1: Why customers trust Sophos

Testing key features

Before you test, here are some items to consider and to compare to competing products:

- Can you manage protection for all your platforms from a single management console?
- How many deployments are required to provide equal endpoint protection coverage – Anti-virus, Anti-spyware, Firewall, HIPS, Application Control, Device Control, Data Control and Network Access Control?
- How easy is the product to install and deploy across the enterprise? Can you use Active Directory (AD) to speed this process?
- Can you synchronize with AD and automatically deploy protection to a new computer as it joins the network?
- How easy is it to assess and control network access for managed and unmanaged computers?
- Does the management console provide a real-time dashboard view of status and alerts?
- How easy is the product to manage? In particular, how many steps and how long does it take to perform common management tasks like amending and applying policies to groups?
- How effective are the proactive detection/HIPS technologies and how much configuration do you have to undertake to enable and maintain effective protection?
- Can the endpoint agent monitor for the transfer of sensitive data to removable storage devices or internet enabled applications like email, web browsers and instant messaging?
- How easy is it to control the usage of removable storage devices and what different enforcement options are available?
- How easy is it to prevent a user from downloading and installing legitimate applications that you don't want them to use on your business network, software such as IM, P2P, VoIP and games? How much work is required to keep the application lists updated with new versions?
- How much of a memory footprint is consumed by the client, and how frequent and large are the protection updates?
- Can you access locally-based and well-trained technical support experts 24x7 without paying extra?

SOPHOS ENTERPRISE CONSOLE

2 SINGLE, CENTRAL AUTOMATED CONSOLE

OVERVIEW OF SOPHOS ENTERPRISE CONSOLE

Sophos Enterprise Console delivers smarter, simpler policy-based management of your endpoint protection. It lets you manage thousands of Windows, Mac, Linux and UNIX computers from a single console.
The console's straightforward management, effortless control over policies across the entire network, scalability, and centralized targeted cleanup, significantly lower recurring management costs.

Many security solutions are over-engineered and can burden you with increasingly complex systems. Enterprise Console has been engineered to give you a simple, integrated approach that allows you to take rapid action against emerging and potential problems. This section highlights the key features of Enterprise Console and details the unique benefits they bring.

SINGLE DEPLOYMENT

Endpoint protection and third party removal

Endpoint Security and Data Protection enables you to deploy and manage the anti-virus, client firewall and compliance control (NAC) components across endpoint computers, from one console.

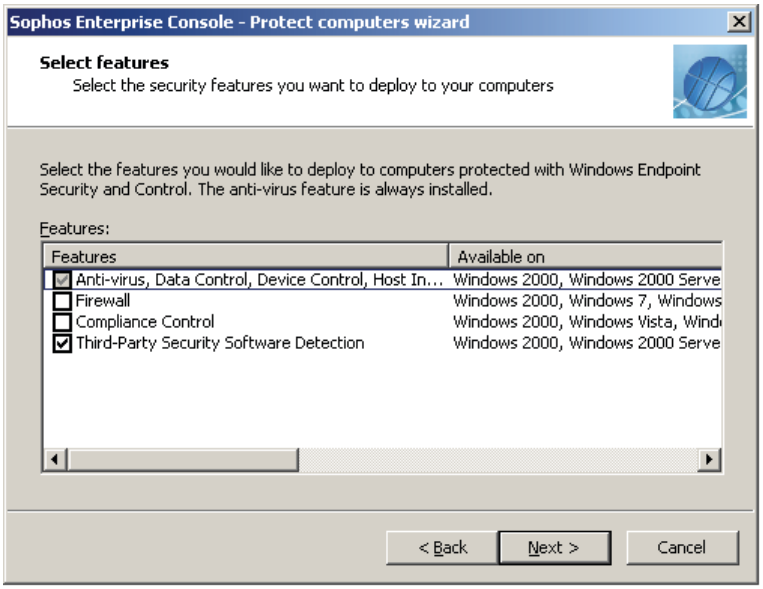

Sophos Enterprise Console - Protect computers wizard
Select features
Select the security features you want to deploy to your computers
Select the features you would like to deploy to computers protected with Windows Endpoint Security and Control. The anti-virus feature is always installed.
Features:
Features
Available on
Anti-virus, Data Control, Device Control, Host In...
Windows 2000, Windows 2000 Serve
Firewall
Windows 2000, Windows 7, Windows
Compliance Control
Windows 2000, Windows Vista, Wind
Third-Party Security Software Detection
Windows 2000, Windows 2000 Serve
< Back
Next >
Cancel

Figure 1: Single deployment

In addition to make moving from your existing solution to Endpoint Security and Data Protection easier we give you the option of removing third-party security software during deployment.

ACTIVE DIRECTORY INTEGRATION AND SYNCHRONIZATION

Faster deployment and automatic protection

Sophos Endpoint Security and Data Protection makes it easy to find computers on your network by enabling the replication of Active Directory groups and client structure into Enterprise Console.

Following replication, you can choose to synchronize Active Directory with Enterprise Console so that any changes in Active Directory are automatically reflected in Enterprise Console – ensuring automatic protection of new clients as they join the network. Enterprise Console will automatically check for changes in Active Directory every hour by default.

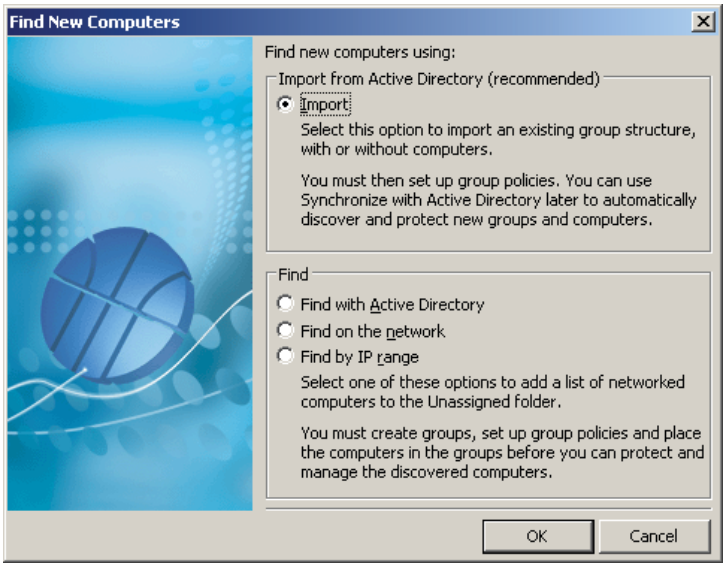

Find New Computers
Find new computers using:
Import from Active Directory (recommended)
Import
Select this option to import an existing group structure, with or without computers.
You must then set up group policies. You can use Synchronize with Active Directory later to automatically discover and protect new groups and computers.
Find
Find with Active Directory
Find on the network
Find by IP range
Select one of these options to add a list of networked computers to the Unassigned folder.
You must create groups, set up group policies and place the computers in the groups before you can protect and manage the discovered computers.
OK
Cancel

Figure 2: Finding new computers quickly

If you are not using Active Directory, there are two alternative methods you can use to quickly identify computers:

- using built-in network find
- searching by IP/Subnet range.

SECURITY DASHBOARD

Greater visibility and automatic alerting

When any virus, spyware, adware, suspicious item, or a potentially unwanted application is detected, an alert is automatically generated and displayed on the dashboard.

Outbreak risk levels across the entire network are displayed on Enterprise Console's security dashboard, which collates all the alerts from Windows, Mac, Linux and UNIX computers and displays the status as Blue (OK), Amber (Warning), or Red (Critical).

At the click of a mouse, you can:

- Filter the view to focus on those computers with out-of-date protection or with malware alerts, giving you instant visibility of the areas on your network that require attention.
- Adjust the dashboard thresholds at which the status colours will change.
- Enable automatic email alerts to be sent when your defined security thresholds are close.

These features mean you don't have to log in to the console to be alerted to potential security issues.

By default, malware alerts are also displayed on the desktop of any computer on which malware, PUAs, or unauthorized applications have been found. Email and SNMP alerts can also be sent to you or specific users if a virus, a PUA, or an error is found on any of the computers in a group. Any viruses detected on the computer will be displayed as hyperlinks, which lead to the relevant entry in the virus library on the Sophos website.

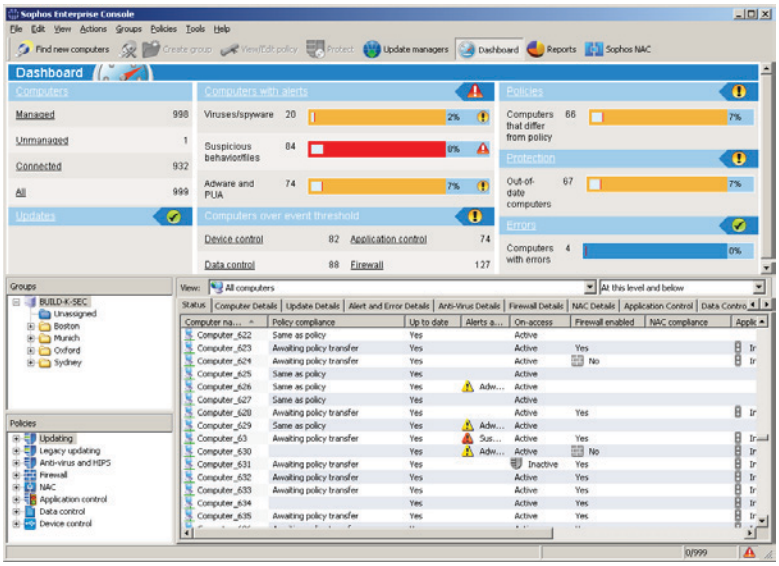


Figure 3: Sophos Enterprise Console security dashboard

At-a-glance dashboard

The ability to view problem areas at a glance is a major advantage, and automatic email alerts are sent when security thresholds are triggered.

Keeping track of critical events

When an application control, firewall, data control, or device control event occurs on an endpoint computer, for example, an application has been blocked by the firewall, that event is sent to Enterprise Console and can be viewed in the respective event viewer.

Using the event viewers, you can quickly and easily investigate events that have occurred on the network. You can also generate a list of events based on a filter you configure, for example, a list of all data control events for the past seven days generated by a certain user.

The number of computers with events over a specified threshold within the last seven days is displayed on the dashboard. You can also set up alerts to be sent to your chosen recipients when an event has occurred.

SMART VIEWS

Targeted cleanup

Cleaning up a large network after an attack can be expensive and time-consuming. Enterprise Console provides remote, centralized cleanup of files, registry entries, and running processes. Smart Views gives a complete view of the security status of all computers on the network from one console, enabling you to view and fix only those computers that need attention, for example those with out-of-date protection or those not complying with policy.

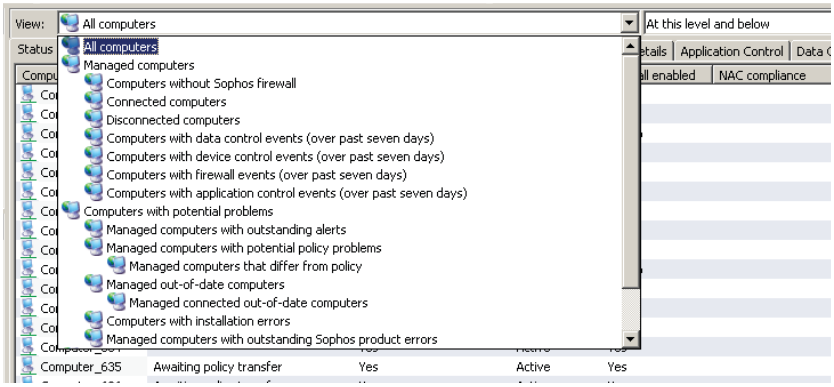


Figure 4: Smart Views

SOPHOS UPDATE MANAGER

Rapid updates, managed from a single point

The Sophos Update Manager ensures that the network is protected at all times with automatic updating of your security software from Sophos. An update manager is installed with and managed from Enterprise Console.

Once you have configured an update manager, it:

- Connects at a scheduled frequency to a data distribution warehouse at Sophos or on your network.
- Downloads the relevant updates for the security software to which the administrator has subscribed.
- Places the updated software in one or more network shares for installation on endpoint computers.

The endpoints will then update automatically from the network shares, in line with the updating policy you configure.

ACTIVEPOLICIES

Simplified policy setting and enforcement

Using Sophos ActivePolicies™, you can quickly and intuitively create and deploy network-wide policies independently of groups, allowing you to deploy one policy across multiple groups simultaneously. ActivePolicies takes the pain out of policy enforcement in seven key areas.

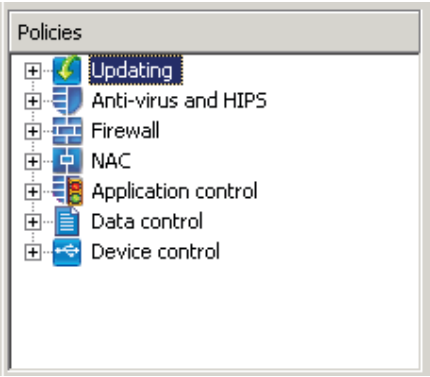


Figure 5: ActivePolicies

Updating policies

Enterprise Console enables you to keep your computers up to date with the latest protection. You can configure the times at which different parts of the network update and the location computers will connect to for their updates. This feature is particularly useful if your organization has large networks covering different time zones, or staff working at their computers at different times – particularly remote laptops connecting to the network. Controlling automatic update settings also enables you to minimize the effect of updates on network performance.

Configuring software subscription settings allows you to specify which versions of endpoint software are downloaded from Sophos for each platform. The default subscription includes the latest software for Windows 2000 and later.

You can also use bandwidth throttling, preventing computers from using all the bandwidth for updating when they need it for other purposes, e.g. downloading email.

Anti-virus and HIPS policies – virus, spyware, PUA, intrusion prevention

Implementing our anti-virus protection also provides you with a complete host intrusion prevention system (HIPS) without the need for complex installation and configuration. It enables runtime analysis, buffer overflow and unique pre-execution protection, proactively detecting malware and suspicious files and behavior.

The policy lets you configure a wide range of scanning options for the entire network. You can specify requirements for on-access, on-demand, scheduled, and web scanning and can opt to exclude particular file types where they are known to pose no threat. By default, computers will use the following standard policy:

- Scan all files that are vulnerable to malware.
- Deny access to any file that contains a virus, spyware, etc.
- Display an alert on the desktop of any computer where a virus or PUA is found.

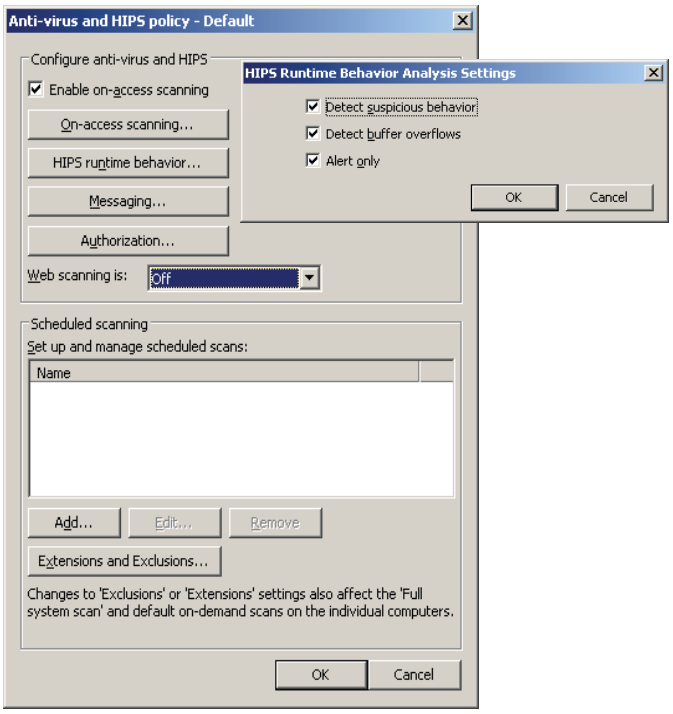


Figure 6: Configuring Anti-virus and HIPS policy

Application control policies

Applications like VoIP, IM and P2P are increasingly the cause of security, legal and productivity issues in business – consequently IT departments are being asked to control their unauthorized installation and usage. Sophos integrates the detection of such controlled applications alongside malware and PUA detection, enabling control without the requirement for the purchase, installation, or management of a separate point product.

All controlled applications are authorized by default, but you can use Enterprise Console to configure policies for groups of endpoint computers to reflect the security requirements for specific locations or departments. For example, VoIP can be switched off for office-based desktop computers, yet authorized for remote computers. To block an application you can simply move the targeted application to the blocked column.

The list of controlled applications is supplied by Sophos and updated regularly. You cannot add new applications to the list, but you can submit a request to Sophos to include a new legitimate application you would like to control on your network.

For a full list of the applications that you can control, please see:
http://www.sophos.com/security/analyses/controlled-applications/

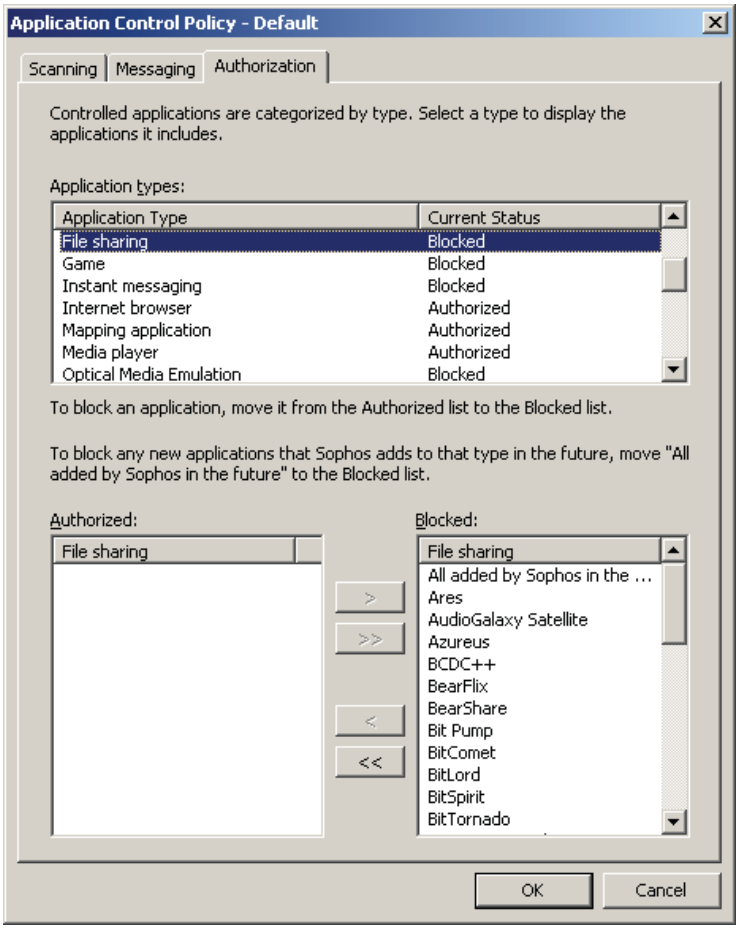


Figure 7: Application control – easy control of unauthorized software

Controllable applications include:

- VoIP
- Instant Messaging
- Peer-to-peer software
- Distributed computing projects
- Search engine toolbars
- Media players
- Internet browsers
- Games (Windows and multi-player games)
- Virtualization applications
- Remote management tools
- Mapping applications
- Email clients
- Online storage
- Encryption tools

Device control policies

Device control can help to significantly reduce your exposure to accidental data loss and restrict the ability of users to introduce software and malware from outside of your network environment.

Integrated into the Sophos endpoint agent, it enables you to control three types of device:

- Storage: Removable storage devices (USB flash drives, PC Card readers, and external hard disk drives); Optical media drives (CD-ROM/DVD/Blu-ray drives); Floppy disk drives; Secure removable storage devices
- Network: Modems; Wireless (Wi-Fi interfaces, 802.11 standard)
- Short Range: Bluetooth interfaces; Infrared (IrDA infrared interfaces)

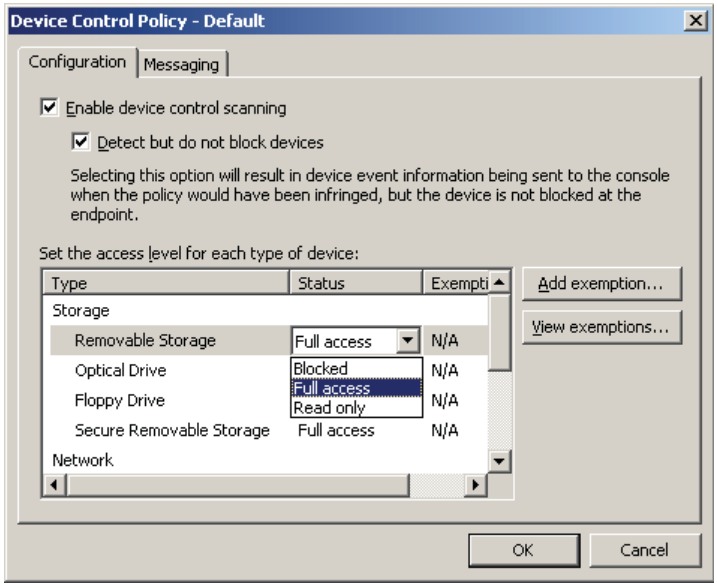


Figure 8: Device control – granular control of removable storage

By default, device control is turned off and all devices are allowed. If you want to enable device control for the first time, Sophos recommends that you:

- Select device types to control.
- Detect devices without blocking them.
- Use device control events to decide which device types to block and which, if any, devices should be exempt.
- Detect and block devices or allow read-only access to storage devices.

Each device type supports both device instance and model exceptions. This means that a USB key which belongs to the IT department can be exempted from the removable storage block policy.

Exceptions are made easy to manage using the device control event viewer within the Sophos Enterprise Console. It enables you to quickly filter and review events generated by the device control policy, and authorize devices by exempting them from the policy.

You can also significantly reduce the risk of network bridging between a corporate network and a non-corporate network. The Block bridged mode is available for both wireless and modem types of device. The mode works by disabling either wireless or modem network adapters when an endpoint is connected to a physical network (typically through an Ethernet connection). Once the endpoint is disconnected from the physical network, the wireless or modem network adapters are seamlessly re-enabled.

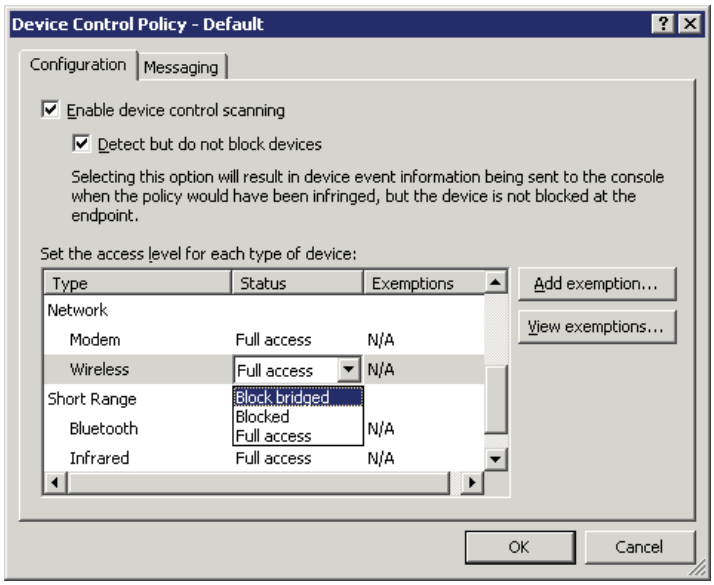


Figure 9: Device control – preventing network bridging

Data control policies

Deploying a stand-alone DLP solution to protect against the accidental loss of sensitive data can be time consuming and costly, and can have a significant impact on the system performance of your endpoints. Sophos removes this pain by integrating the scanning for sensitive information into the endpoint agent, making it easier for you to configure, deploy and manage.

You can monitor and control the transfer of files to specified storage devices (e.g. removable storage device or optical drive) or by specified internet-enabled applications (e.g. email client, web browser or instant messaging) without having to deploy a separate solution and another endpoint agent.

Sophos provides a number of preconfigured data control rules covering national identification numbers to confidential document markers. You can use these rules out of the box or tailor to meet your own needs.

There are two types of data control rule:

- file matching rule: specifies the action that is taken if the user attempts to transfer a file with the specified file name or of the specified file type (true file type category, e.g. a spreadsheet) to the specified destination, for example, block the transfer of databases to removable storage devices
- content rule: contains one or more data definitions and specifies the action that is taken if the user attempts to transfer data that matches all the definitions in the rule to the specified destination.

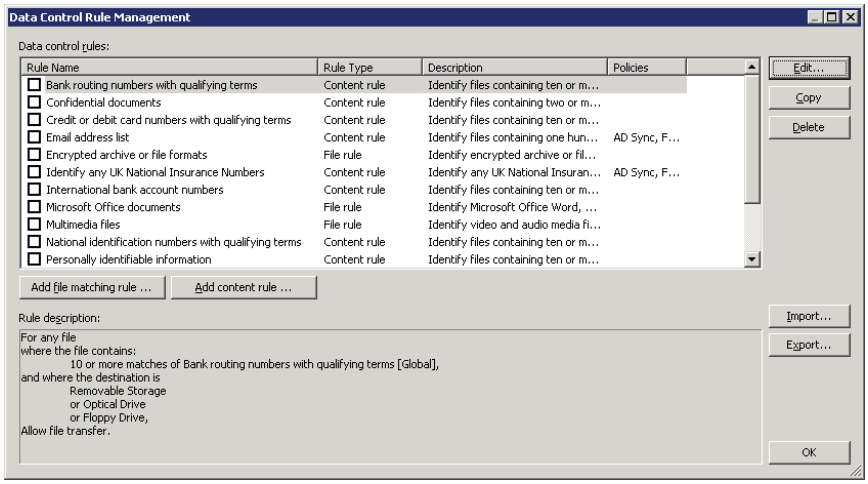


Figure 10: Data control – preconfigured policy rules

To simplify policy creation, SophosLabs maintain a library of extensive library of global sensitive data definitions (Content Control Lists) which covers personally identifiable information (PII) such as credit card numbers, social security numbers, postal addresses, or email addresses.

These definitions use a wide range of techniques to ensure accurate detection. They are continually refined by SophosLabs and new definitions will be added as part of the monthly endpoint data updates.

You can create your own lists specific to your organization such as customer reference numbers or specific confidential document markers.

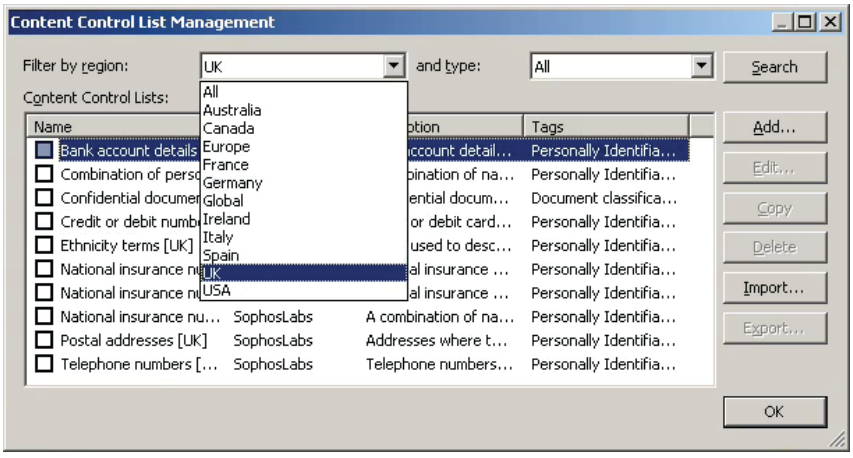


Figure 11: Data control – Content Control Lists

There are a number of actions that can be taken when a data control rule is matched:

- Allow file transfer and log event
- Allow transfer on acceptance by user and log event
- Block transfer and log event

By default, when a rule is matched and file transfer is blocked or user confirmation of file transfer is required, a message will be displayed on the endpoint computer's desktop. You can easily add your own custom messages to the standard messages for user confirmation of file transfer and for blocked file transfer.

The "authorize transfer on user acceptance" action can be used to train users that the data they are transferring may contravene a company policy without actually preventing them from carrying out their work. The end users decision is audited and can be reviewed at a later date.

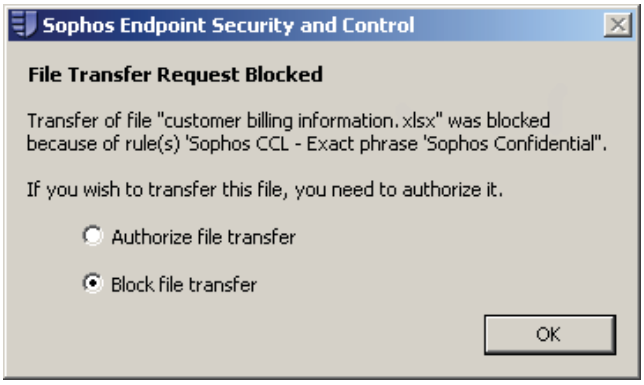

Sophos Endpoint Security and Control
File Transfer Request Blocked
Transfer of file "customer billing information.xlsx" was blocked because of rule(s) 'Sophos CCL - Exact phrase 'Sophos Confidential".
If you wish to transfer this file, you need to authorize it.
Authorize file transfer
Block file transfer
OK

Figure 12: Data control – End user authorization notification

When a data control event occurs, for example, the copying of a file containing sensitive data to a USB flash drive, the event is sent to Enterprise Console and can be viewed in the data control event viewer. The number of computers with data control events over a specified threshold within the last seven days will also be displayed on the dashboard.

Firewall policies

By default, Sophos Client Firewall is enabled for all computers in all groups and blocks all non-essential traffic. It is shipped with a set of secure default policies, but you can easily change these to suit your particular business requirements. Every aspect of the firewall configuration can be centrally managed (please see section 3 for more on Sophos Client Firewall).

The "alert only" mode allows you to deploy the firewall across your estate to collect information on all applications that are used on the network. This information will be sent back to the console and you can use this to build a policy that won't impact your users' productivity, before you roll out a "live" policy.

You can configure different location aware security policies to ensure that mobile computers are protected, whether in or out of the office. The location of the mobile computer is detected using either DNS or the gateway MAC address.

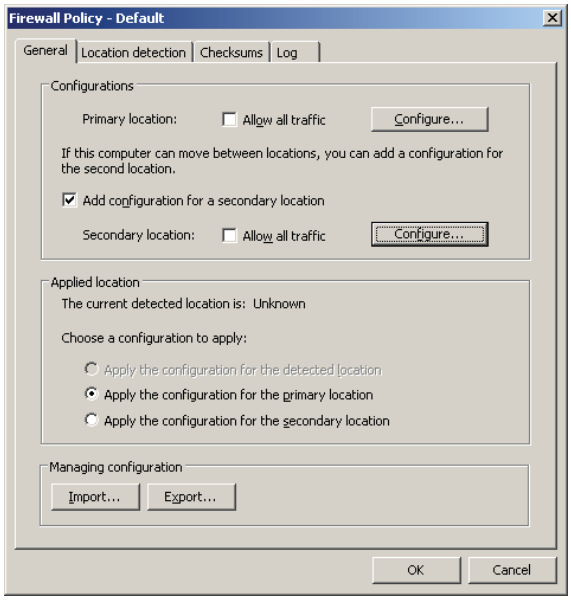


Figure 13: Location aware firewall

Network access control policies

NAC policies are controlled through the NAC Manager which is launched from the NAC menu button at the top of the console, or by double clicking on a NAC policy.

Endpoint Security and Data Protection comes pre-configured with policies for managed and unmanaged computers. The NAC Manager provides additional policy editing, reporting, access control, and system configuration capabilities and is divided into four main functional navigation areas: Manage, Enforce, Report, and Configure system.

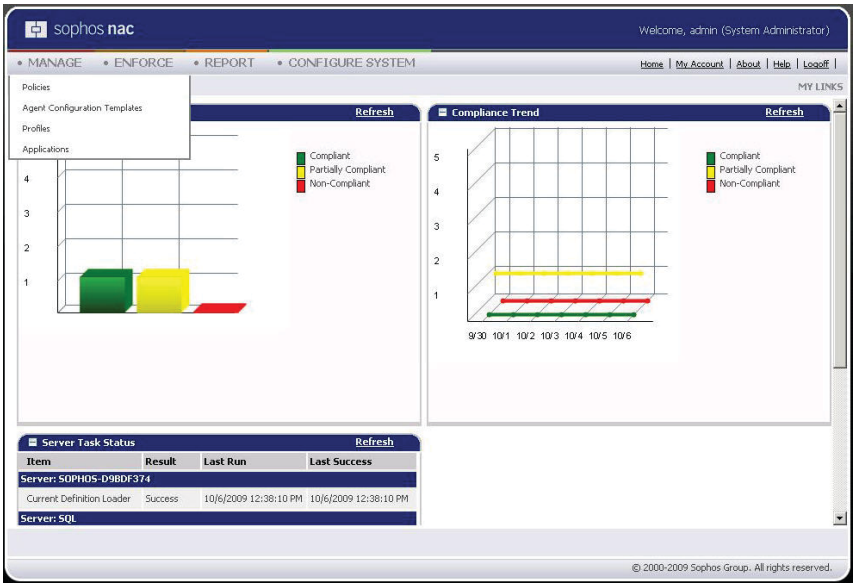


Figure 14: NAC management user interface provides an at-a-glance view of compliance across the network

Important

Assessment and control of unmanaged/unauthorized computers requires the installation of the Sophos DHCP server component on a Microsoft DHCP server. It is recommended the network administrator responsible for Microsoft DHCP is involved in this process.

- Manage—provides components for editing and managing policies and managing computers.
- Enforce—offers control of network access using access templates and exemptions.
- Report—offers a suite of reports for troubleshooting compliance and network access.
- Configure — provides control over components required for system management, configuration and server settings.

After logging in, you are provided with an immediate view of your organization's overall compliance. The current compliance chart provides an instant view of how many computers on the network are compliant with your security policy and how many are partially compliant and non-compliant. A second chart shows the recent compliance trend.

Pre-defined policies for managed and unmanaged computers

Policies enable you to control access of specific groups to network resources based on the security evaluation of each user's individual computer. They also determine the compliance state of the computer, messages that are displayed, remediation actions that are performed, and enforcement actions that are taken.

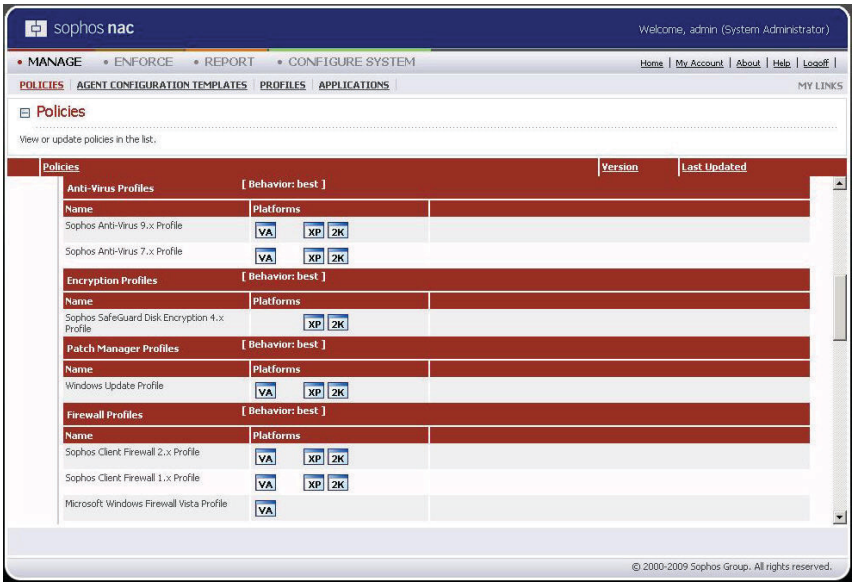

sophos nac
Welcome, admin (System Administrator)
MANAGE
ENFORCE
REPORT
CONFIGURE SYSTEM
Home | My Account | About | Help | Logoff |
POLICIES | AGENT CONFIGURATION TEMPLATES | PROFILES | APPLICATIONS
MY LINKS
Policies
View or update policies in the list.
Policies
Version
Last Updated
Anti-Virus Profiles [Behavior: best]
Name
Platforms
Sophos Anti-Virus 9.x Profile
Sophos Anti-Virus 7.x Profile
Encryption Profiles [Behavior: best]
Sophos SafeGuard Disk Encryption 4.x Profile
Patch Manager Profiles [Behavior: best]
Windows Update Profile
Firewall Profiles [Behavior: best]
Sophos Client Firewall 2.x Profile
Sophos Client Firewall 1.x Profile
Microsoft Windows Firewall Vista Profile
© 2000-2009 Sophos Group. All rights reserved.

Figure 15: Pre-configured policies allow computers to be assessed for security compliance

There are three pre-defined NAC policies:

- **Default**—The default policy is designed so you can quickly assess and control managed clients. All new Enterprise Console groups and any client with no policy assigned to it, or that cannot find the policy assigned to it, will pick up the default policy. This default policy is pre-populated with Sophos Anti-Virus, Sophos SafeGuard Encryption, Sophos Client Firewall, Microsoft/Windows Update and MS Windows Firewall XP SP2/Vista.
- **Managed**—The managed policy is identical to the default policy. This allows you to make changes to one of these policies and test it before assigning it to your machines.
- **Unmanaged**—The unmanaged policy is applied to those computers that temporarily join the network and are assessed with the Java-based dissolvable agent. It is pre-configured to assess a range of third-party security products including popular anti-spyware, anti-virus and firewall applications and Windows or Microsoft Update. Vendors include Sophos, Microsoft, Trend Micro, McAfee, Symantec/Norton, F-Secure, Panda, Spybot and Ad-Aware and more.

Important

To fully evaluate the Sophos NAC functionality please download and install the NAC Manager component from www.sophos.com/downloads/ (Your evaluation credentials will provide you with access to this area.)

MESSAGE RELAYS

Significant scalability

Sophos Endpoint Security and Data Protection has been engineered to be highly scalable, so you can manage tens of thousands of computers from a single console. Even greater scalability is achieved with message relays that allow computers on the network to act as relays to Enterprise Console. This feature reduces network traffic and load on the management server and lets very large organizations manage tens of thousands of computers.

REPORTS

Customized and scheduled reporting

On-demand, integrated, network-wide reporting is pivotal to maintaining security. The Enterprise Console provides a number of reports textual and graphical information on a variety of aspects of your network's security status. These can be used out of the box or easily configured to suit your needs. Standard report types include:

- Alerts by item name
- Alerts per location
- Alerts by time
- Alert history
- Alerts summary
- Endpoint policy non-compliance
- Managed endpoint protection
- Updating hierarchy
- Events per user

Reports can be output in table format as well as chart format, including pie charts and can be exported in a number of file formats, namely: PDF (Acrobat), HTML, MS Excel, MS Word, RTF, CSV, XML.

Using the Report Manager, you can quickly create a report based on an existing template, change configuration of an existing report, and schedule a report to run at a specific time and with a repeat frequency – run once, daily, weekly, monthly – and have the results automatically emailed to selected recipients.

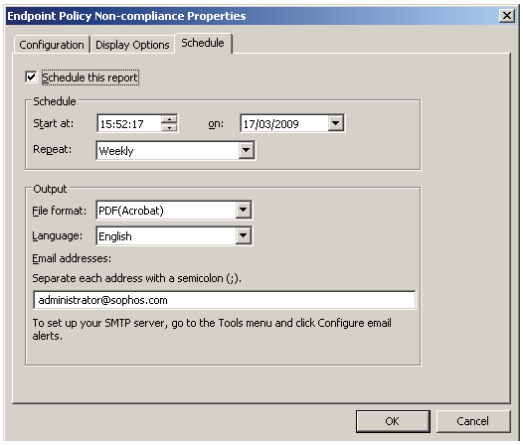


Figure 16: Scheduling of reports

Additional reporting enables you to view information about any individual computer. Double-clicking on the computer's name will bring up a dialog box showing details, such as IP address, username and last scan date.

ROLE-BASED ADMINISTRATION

Devolving management to ease the administrative workload

The combination of configurable roles, rights and sub-estates in Endpoint Security and Data Protection enables flexibility in administrating security across your entire estate.

With role-based administration, you can configure access to the Enterprise Console, allowing you to share the administration with specific teams or individuals, by using the preconfigured roles or creating your own roles. For example, a Help Desk engineer can update or clean up computers, but cannot configure policies, which is the responsibility of an Administrator.

To configure access, you simply set up the required roles, add specific rights and then assign Windows users and groups to the relevant roles.

There are four pre-configured roles:

1. **System Administrator**—A pre-configured role that has full rights to manage Sophos security software on the network and roles in Enterprise Console. The System Administrator role cannot be edited or deleted.
2. **Administrator**—A pre-configured role that has rights to manage Sophos security software on the network, but cannot manage roles in Enterprise Console. The Administrator role can be renamed, edited, or deleted.
3. **Helpdesk**—A pre-configured role that has remediation rights only, for example, to clean up or update computers. The Helpdesk role can be renamed, edited, or deleted.
4. **Guest**—A pre-configured role that has read-only access to Enterprise Console. The Guest role can be renamed, edited, or deleted.

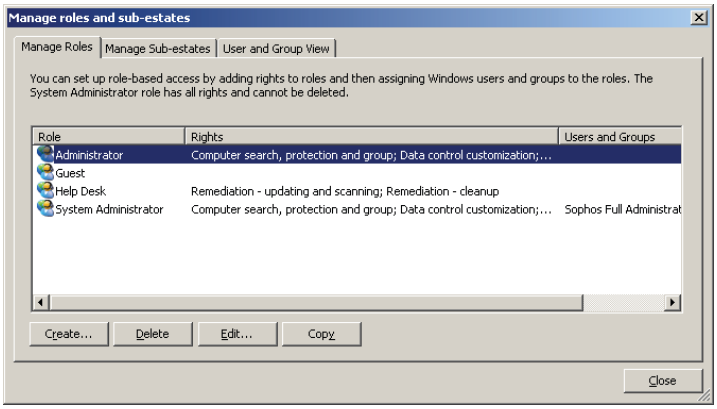

Manage roles and sub-estates
Manage Roles
Manage Sub-estates
User and Group View
You can set up role-based access by adding rights to roles and then assigning Windows users and groups to the roles. The System Administrator role has all rights and cannot be deleted.
Role
Rights
Users and Groups
Administrator
Computer search, protection and group; Data control customization;...
Guest
Help Desk
Remediation - updating and scanning; Remediation - cleanup
System Administrator
Computer search, protection and group; Data control customization;...
Sophos Full Administrat
Create...
Delete
Edit...
Copy
Close

Figure 17: Managing role-based administration

Sub-estate Management

By splitting your IT estate into sub-estates, you can also restrict the computers and groups that users can perform operations on.

You can control access to the sub-estates by assigning Windows users and groups to them. A user can only see the groups and machines relevant to their sub-estate.

Reports are also specific to the sub-estate. Any policies will only be applicable to the sub-estate in which they were created; an administrator cannot change policies that are applicable outside of their sub-estate.

For reporting, administrators can only configure and run reports applicable to their own sub-estate. A full system administrator can run reports across the entire IT estate.

SCALABLE INFORMATION STORAGE

Microsoft SQL Server integration

Enterprise Console integrates as standard with MSDE (Microsoft SQL Server Desktop Engine) to store management information. If your organization is large, you might wish to use Microsoft SQL Server, which has enhanced functionality and greater scalability for large networks.

SOPHOS ENDPOINT SECURITY AND DATA PROTECTION

3 PROTECTING WINDOWS COMPUTERS

Sophos Endpoint Security and Data Protection protects your Windows network with Sophos Endpoint Security and Control for Windows, Sophos NAC, SafeGuard Disk Encryption and Sophos Client Firewall.

SOPHOS ENDPOINT SECURITY AND CONTROL FOR WINDOWS

Designed for corporate networks, Sophos provides more than just protection against malware, incorporating our host intrusion prevention system (HIPS) plus control of removable storage devices, unauthorized applications and the transfer of sensitive data.

The single endpoint agent eliminates your reliance on separate standalone products, delivering:

- Anti-virus and HIPS (blocking Viruses, spyware, adware and PUAs, suspicious files and behaviour)
- Application control (preventing the installation and usage of unauthorized applications)
- Device control (managing the use of removable storage devices and wireless networking protocols
- Data control (scanning for the transfer of sensitive data off the endpoint)
- Client firewall (protecting against hackers and unauthorized application communication)

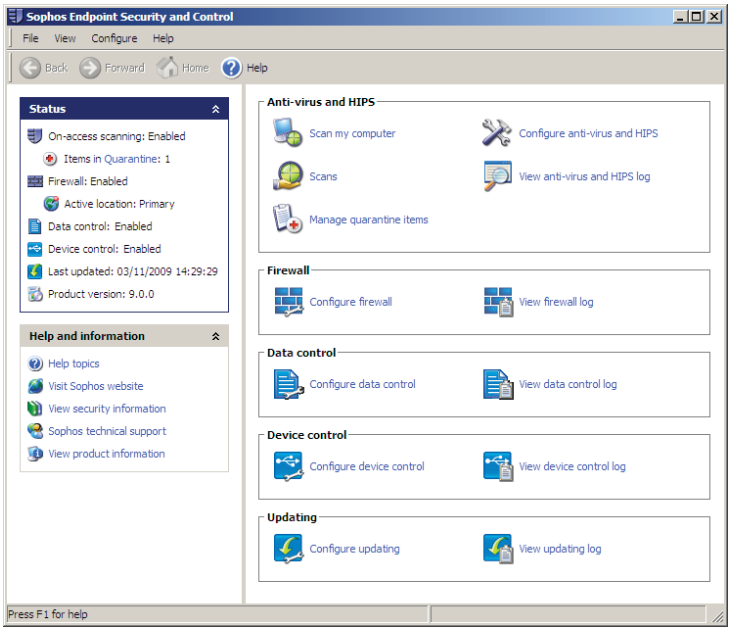


Figure 18: Single endpoint agent significantly lowers impact on system performance

Intrusion prevention

Sophos Endpoint Security and Control for Windows includes complete intrusion prevention (HIPS), ensuring proactive protection without you having to carry out the complex installation and configuration of a separate product. A number of pre-emptive detection technologies combine to ensure your network is secure against today's blended and targeted zero-day threats:

- **Genotype® technology** provides zero-day protection, recognizing families and variants of known viruses, enabling them to be pre-emptively blocked even before specific detection becomes available
- **Behavioral Genotype® Protection** automatically guards against new and targeted threats by analyzing behavior before code executes
- **Built-in HIPS technologies** including pre-execution suspicious file detection, runtime suspicious behavior analysis and buffer overflow protection, all combine to detect malware, suspicious files and behavior.

Faster scanning with Decision Caching

Decision Caching™ – the high-performance on-access scanning technology in Sophos Endpoint Security and Control for Windows – optimizes performance by ensuring that only new or changed files are scanned for threats. In addition, intelligent file recognition technology means that only those files which are capable of containing malware are scanned. Remote users can perform on-demand scans of individual files or the whole computer before reconnecting to the main network, providing an extra layer of security.

Quarantine Manager

Quarantine Manager allows the moving or deletion of infected files and lets you selectively block PUAs and controlled applications.

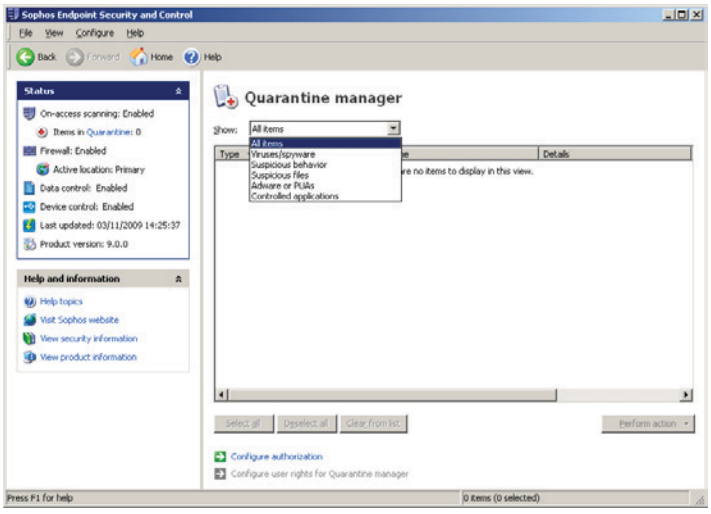


Figure 19: Quarantine manager

Application Control

While some applications can provide efficiency gains, others can distract users from their business tasks, and waste valuable network bandwidth and processing power. In addition, with P2P and IM-based malware attacks growing fast, and regulations that make it a legal requirement to maintain and protect data, the need to control the installation of unauthorized applications is increasingly important.

Sophos integrates application control into the endpoint agent, letting you authorize or block applications selectively, at the desktop level or centrally. You can also block or authorize applications for different groups of computers using ActivePolicies in Sophos Enterprise Console (see chapter 2). For example, you can block VoIP for office-based desktop computers, but authorize it for remote computers.

Device Control

Our device control technology helps you to reduce the risk of data loss and malware infection, by giving you control over removable storage devices and wireless networking prototcols.

Built into the single endpoint agent, it is port agnostic and supports any port used to connect the device including USB, FireWire, SATA and PCMIA interfaces.

Initially the device control policy can be put into a notification only mode enabling you to get a view of device usage across your estate without blocking any devices, before configuring and deploying a control policy to relevant groups.

Each device type can either be authorized (the default setting) or blocked. Storage devices can also be set to "read only" mode, which means that data can be read from the device but not written to it. This can be particularly useful for USB flash disks and CD / DVD drives.

For network interfaces, a "Block bridging" mode prevents network bridging and will disable a computer's wireless interface when the computer has a physical connection to the network, e.g. via an Ethernet cable. Once the cable is disconnected, the wireless interface will be enabled.

Data Control

Sophos is the first vendor to integrate DLP content scanning into the endpoint agent, reducing the impact on system performance with a single agent that scans for sensitive data as well as malware and making it easier for you to configure, deploy and manage.

It enables you to monitor for when users transfer sensitive data, such as Personally Identifiable Information (PII) or company confidential documents to removable storage devices or internet-enabled applications, helping you to prevent the accidental loss of data.

Policy configuration is easy with a number of preconfigured data control rules that you can use out of the box or modify to tailor to your own needs.

SophosLabs also maintains a library of extensive library of global sensitive data definitions (Content Control Lists) which covers personally identifiable information (PII) such as credit card numbers, social security numbers, postal addresses, or email addresses helping you to protect your sensitive data faster.

You can create your own lists specific to your organization such as customer reference numbers or specific confidential document markers.

SOPHOS NAC

Assess and control your Windows endpoints

Computers attempting to connect to the network are assessed for compliance by Sophos NAC against a defined security policy. This endpoint compliance functionality allows you to ensure that all computers are properly protected by:

- Checking if anti-virus and other security applications are correctly configured and up to date.
- Checking if Microsoft Windows operating system service packs are up to date.
- Checking if Microsoft Windows and/or Microsoft Update is active.
- Includes separate policies that can be configured for managed, contractor and guest computers.

Enforcement options to control network access

Sophos NAC uses agent-based enforcement for control of managed computers and interoperates directly with Microsoft DHCP to prevent unmanaged/ unauthorized computers accessing the network. Endpoint assessment is performed by:

- The Sophos NAC Compliance Quarantine Agent (resident on the client)
- The Sophos NAC Compliance Dissolvable Agent (downloadable Java component)

The Sophos NAC Compliance Quarantine Agent, which is deployed from within Sophos Enterprise Console, provides assessment and control of managed computers, both prior to and during a network session, at an interval that can be specified by you. This agent provides self-quarantine for non-compliant computers.

The Sophos NAC Compliance Dissolvable Agent provides the same assessment prior to network access for LAN-based unmanaged computers. It is designed for users who do not or cannot have an agent installed on the endpoint, yet who must still access specific network resources, such as contractors or guests. Sophos NAC provides integration with Microsoft DHCP to protect the network from LAN-connected computers by using an enterprise's existing Microsoft DHCP infrastructure, allowing Sophos NAC to quarantine non-compliant and unauthorized computers.

SAFEGUARD DISK ENCRYPTION

SafeGuard Disk Encryption is an easy to implement solution that encrypts hard disks and data on mobile media to protect against the loss of data and meet compliance requirements.

Securing data through full disk encryption

Hard disks (IDE, SCSI, serial ATA) are encrypted at sector level, which means that the entire content including any operating systems, temporary files, swap files or "hibernation" files are encrypted. Since encryption takes place at sector level, it is entirely transparent for users. As information is written to and read from the disk it is automatically encrypted and decrypted without requiring user intervention.

Easy deployment across the network

SafeGuard Disk Encryption is easy to implement on standalone machines or unattended across your network. The straightforward configuration wizard allows you to quickly create a configuration file which can then be installed and distributed using existing tools. Even the initial encryption of the hard disk(s) can be carried out without direct intervention from either administrators or users, and there is no burden on the administrator to set up any management infrastructure.

Securing the operating system

The Pre-Boot Authentication (PBA) process cannot be circumvented and requires a password before the operating system starts. The enciphering key is not stored on the hard disk, but is dynamically generated from the password. Once the password has been authenticated, the user will then be signed through into Windows.

Resetting forgotten passwords

If users forget their login passwords, they are unable to logon. Should this occur, the administrator can simply use the Response Code Wizard to assign a secure new SafeGuard password to the user.

SOPHOS CLIENT FIREWALL

Sophos Client Firewall is integrated into the endpoint agent making deployment, configuration, updating, and management by Enterprise Console simple. It proactively locks down computers, protecting against known and unknown threats, such as internet worms, hackers, and unauthorized application communication. Features that prevent application hijacking and impersonation ensure Sophos Client Firewall delivers better protection than the simple port blocking firewalls offered by many other security vendors.

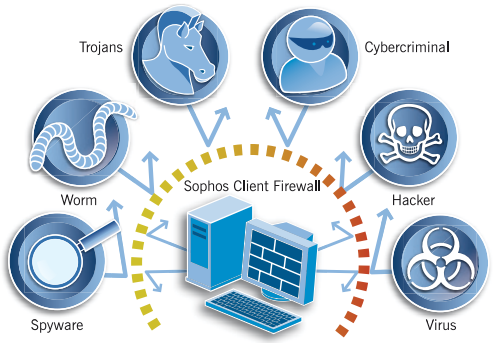


Figure 20: Zero-day protection

Zero-day protection against known and unknown threats

Sophos Client Firewall provides zero-day protection, i.e. it blocks the window of vulnerability that exists between a new threat emerging and protection being deployed. It defends all corporate computers from complex and rapidly spreading threats and prevents outbreaks before they can disrupt business continuity.

Proactive lockdown

Sophos Client Firewall protects against network and internet worms, hackers, and the risk of unprotected computers connecting to the network, by proactively locking down computers—both those in the office and laptops connecting via wireless hotspots and hotel broadband connections.

Port tracking and blocking to eliminate threats

Sophos Client Firewall stops known and unknown threats by tracking active ports and closing all inactive ports, ensuring that internet worms and hackers are blocked.

Stealth technology – preventing intrusion by hackers

Cybercriminals, such as hackers, use port scanning to identify and target vulnerable computers with open ports. They do this by sending out connection requests across the internet. Sophos's stealth technology prevents computers from responding to these requests, hiding a computer and making it appear inactive to the outside world. This gives you an additional level of protection, ensuring privacy by eliminating the opportunity for hackers to identify and target vulnerable computers.

Ensuring protection with location awareness

Sophos Client Firewall lets you configure different policies for different locations according to the location where computers are used, for example, in the office (on the network) and out of the office. The Enterprise Console will then apply different firewall settings to the computers depending on whether they are on the network or not. This dual location configuration is particularly important for mobile computers such as laptops.

Preventing application hijacking and impersonation

Application-level filtering is used to monitor application behavior, allowing internet or network access only to applications that meet your specifications. Sophos Client Firewall prevents application hijacking by monitoring inappropriate application and system calls, and the launching of hidden processes. It also uses a checksum method to foil attempts by spyware and other malware to masquerade as a legitimate application, thereby preventing the theft of confidential information over the internet.

Stateful inspection scans incoming and outgoing data packets

Sophos Client Firewall uses stateful inspection to enhance security by keeping track of packets to ensure only legitimate packets are allowed. Packets are tracked in order to allow limited response communication. For example if an outbound packet is sent then only those incoming packets originating from the computer that has been communicated with (from the appropriate port) are allowed through the firewall.

Central reporting and logging

The firewall provides a central report to the management console. This includes unknown applications and traffic, hidden processes and modified memory events. This provides a simple way for you to understand potential areas of security concern. In addition, the firewall's log viewer lets you view, filter, and save details of the connections that the firewall has allowed or blocked.

Monitor-only mode

The firewall can be deployed across your entire estate in an "alert only" mode. It will discover all applications that are used on the network (taking into account any LAN settings you have made). The results are reported back to the Enterprise Console. This allows you to collect information about unknown traffic and then to refine firewall policies accordingly without impacting user productivity.

Interactive working

The firewall can run in a learning (interactive) mode, asking the user how to deal with detected traffic. If this mode is enable, the firewall will display a pop-up on the endpoint computer each time an unknown application or service requests network access. The learning dialog asks the user whether to allow or block the traffic, or whether to create a rule for that type of traffic.

SOPHOS ANTI-VIRUS FOR MAC OS X, LINUX AND UNIX

4 PROTECTING NON-WINDOWS COMPUTERS

THE NEED TO PROTECT NON-WINDOWS COMPUTERS

It has become increasingly important to protect Mac, Linux, UNIX and other computers. The ability of non-Windows computers to harbor and spread Windows viruses, the occasional appearance of targeted Mac and Linux viruses, and legal demands that every computer be protected, all place an increasingly heavy burden on your shoulders.

Sophos Anti-Virus for Mac OS X and Sophos Anti-Virus for Linux, and Sophos Anti-Virus for UNIX offer a powerful, intuitive solution designed for corporate servers, desktops, and laptops.

SOPHOS ANTI-VIRUS FOR MAC OS X

Sophos Anti-Virus for Mac OS X detects viruses, spyware, Trojans, and worms in real time and on demand, and automatically cleans Windows as well as Mac malware. Sophos Anti-Virus for Mac OS X also detects viruses in compressed attachments, including recursive archives.

Management control from either Mac or Windows platform

Sophos Anti-Virus for Mac can be managed either by using Sophos Update Manager for Mac or Sophos Enterprise Console (Windows). You do not need to run both of these administrator interfaces to ensure that Sophos Anti-Virus for Mac OS X is kept up to date

Centralized management

Enterprise Console enables you to configure and manage anti-malware protection for Windows, Mac, Linux and UNIX computers, network-wide from a central point. Enterprise Console does require a Windows computer to be available and offers enhanced management functionality.

If you are on a Mac only network, then Sophos Update Manager for Mac allows updating and configuration from a single Mac computer. It enables you to set automatic updating and choose how you receive email notifications. You can also determine how scanning will be implemented on Mac desktops and laptops, and enables full centralized configuration of the desktop settings

Automatic updating from SophosLabs

You can use either Sophos Enterprise Console or Sophos Update Manager for Mac OS X to manage updating software and protection.

You can specify the address, username, and password needed for computers to update themselves with the latest virus identity files (IDEs) from SophosLabs. Alternatively, you can set computers to update themselves from the CID (the central installation directory, which is set up on the network during the install process).

You can also enable remote and mobile users to update from wherever they are via the network or internet, either from the main server, a backup, or directly from Sophos.

Automatic reporting of virus incidents

Enterprise Console's security dashboard shows outbreak risk data, and automatic email alerts are sent when outbreaks occur, enabling you to take early action.

Using Sophos Update Manager for Mac, you can also set alert options based on immediate scanning and on-access scanning results. Naturally, you can select the recipient of the message. Alerts are stored if the sender is not connected, and are forwarded when the sender reconnects to the network, so that none are lost.

Minimized scanning overheads

Sophos Anti-Virus scans files on access and on demand, intelligently recognizing uninfectable file types, thus saving system resources.

You can set a number of scanning options in Sophos Update Manager, such as excluding certain files from scanning, and setting preferences for actions to take if a threat is found, e.g. disinfect or delete.

SOPHOS ANTI-VIRUS FOR LINUX

Sophos Anti-Virus for Linux provides superior on-access scanning for Linux desktops, laptops and servers, delivering excellent performance, stability and reliability, along with out-of-the-box support for the widest range of Linux distributions.

Central management

Linux computers can be managed by Enterprise Console. The security dashboard shows outbreak risk data, and automatic email alerts are sent when your chosen security thresholds are threatened. Every virus incident is automatically reported, making day-to-day management even easier.

Fast deployment on Linux-only networks

Red Hat Package Manager can be used for deployment in Linux-only environments and configuration and updating can be performed either remotely through a web GUI or the command line interface.

Get performance, stability and reliability

Talpa, Sophos's unique file intercepting module, delivers superior protection by enabling on-access, on-demand and scheduled scanning of local hard disks, media drives, shared-file systems (such as NFS and Samba) and distributed-file systems. The widest range of Linux kernels are supported out-of-the- box, including recent 64-bit versions. This allows you to change, upgrade and compile versions when required, ensuring maximum protection.

Automatic updates

Updates are automatically downloaded and distributed through Enterprise Console, cascading web servers or directly from Sophos, ensuring that all computers across the network, including remote laptops, are fully protected.

SOPHOS ANTI-VIRUS FOR UNIX

Sophos Anti-Virus for UNIX provides integrated cross-platform virus and spyware detection on UNIX servers, desktops and laptops. The powerful detection engine scans all potential entry points for full network protection.

Easy management options

Sophos Anti-Virus for UNIX can be managed from the command line or through Enterprise Console for Solaris 9 and 10 on SPARC and Intel (i386) and HP-UX on Itanium 2, giving you the flexibility you need.

High performance scanning

Scanning and disinfection can be performed on demand and automatically at scheduled times, resulting in a minimum impact on system performance. Decision Caching™ technology means that only those files that have changed are rescanned, resulting in faster scanning with minimum impact on system performance.

Zero-day threats detected before they execute

Behavioral Genotype® Protection automatically guards against unknown threats by analyzing behavior before code executes, delivering the benefits of a Host Intrusion Prevention System (HIPS).

Automated and customized reporting

Every virus incident is automatically reported to the administrator, making day-to-day management even easier.

APPENDIX I

EVALUATING ENDPOINT SECURITY AND DATA PROTECTION

We want you to be absolutely convinced that Sophos Endpoint Security and Data Protection will protect your network and support you better than any other security vendor. This appendix gives you details of what documentation you will need to evaluate our software, suggests a test network and gives you a comprehensive checklist to help you consider every aspect of the software and support we offer.

Startup guide and user manuals

Before you evaluate Sophos Endpoint Security and Data Protection, you will need to download the network startup guide. To find this, go to:

http://www.sophos.com/support/docs/Endpoint_Security_Control-all.html

TEST NETWORK

Sophos supports many platforms, including UNIX, Linux and NetWare. However, to evaluate the centralized management features of Enterprise Console you will need at least one Windows computer. We suggest you include the following in your test network:

- A management console, i.e. a computer running Windows 2000/XP/2003.
- At least one client – we recommend using a Windows 2000/XP/2003/ Vista/7 desktop.

You will also need access to the internet. You might also like to include computers supporting Mac OS X, Linux and UNIX platforms in your test network, as well as a remote standalone computer to evaluate remote updating.

Important

If you have any other anti-virus software installed on your test network, you should uninstall it first. If you have problems doing this, please contact Sophos technical support – contact details can be found at www.sophos.com/support/queries

SYSTEM REQUIREMENTS

For full details, visit www.sophos.com/products/all-sysreqs.html

Enterprise Console system requirements

Platforms supported	Windows 95/98/NT4/2000/XP/2003/Vista/2008/7 Mac OS X Linux UNIX
Hardware	Minimum 2.0 GHz Pentium or equivalent
Management server	Windows Server 2008 Windows Server 2003 and R2 Windows 2000 Server VMWare ESX VMWare Workstation VMWare Server
Sophos NAC management server	Windows Server 2008 32-bit Windows Server 2003 and R2 32 bit
Remote console	Windows Server 2008 Windows Server 2008 and R2 Vista Windows XP Professional Windows 2000 Professional or Server VMWare ESX VMWare Workstation VMWare Server
Disk space	Minimum 150MB MSDE 2 GB SQL 2005 No limit SQL 2008 No limit SQL 2005 Express Edition 4 GB SQL 2008 Express Edition 4 GB SQL Server 2000 2 GB
Memory	Minimum 512 MB Minimum 1 GB if running Sophos NAC Manager

Sophos NAC Compliance Agent system requirements

Platforms supported	Windows 2000/XP/Vista
Disk space	Minimum 20 MB
Memory	Recommended 512 MB RAM

Sophos SafeGuard Disk Encryption system requirements

Platforms supported	Windows 2000/XP
Disk space	Minimum 25 MB
Memory	Recommended 512 MB

Sophos Endpoint Security and Control for Windows system requirements

Platforms supported	
Windows 95/98/NT4/2000 and 2000 Pro/XP Home and Pro/2003/Vista/2008/7 Windows Netbooks Windows XPe Windows Embedded Standard WePOS VMWare ESX VMWare Workstation VMWare Server	
Disk space	
Windows 2000/XP/2003/Vista/2008/7	Minimum 120 MB
Windows Me/98/95/NT4	Minimum 90 MB
Memory	
Windows 2000/XP/2003/Vista/2008 and Enterprise Console	Recommended 256 MB
Windows Me/98/95	Recommended 64 MB
Windows NT4	Recommended 256 MB

Sophos Client Firewall system requirements

Platforms supported	Windows 2000 Pro/ XP Home and Pro/ Vista/7
Disk space	Minimum 100 MB free
Memory	Recommended 320 MB RAM
Processor	Pentium class 300 MHz

Sophos Anti-Virus for Mac OS X test network

You will need to set up a test network of computers running Mac OS X. You will also need to nominate one computer to act as a server containing the central installation directory (CID) – a folder used to download Sophos Anti-Virus and deploy it to the rest of the network. The CID will also house Sophos Update Manager, which keeps Mac OS X computers on the network up to date with the latest virus identity files (IDEs) and configuration settings.

Sophos Anti-Virus for Mac OS X system requirements

Platforms supported	Mac OS X 10.2 or higher
Disk space	Minimum 90 MB free
Memory	Recommended 128 MB RAM
Processor	Intel-based and PowerPC-based Macs

APPENDIX II

THE EICAR TEST “VIRUS”

ABOUT THE EICAR TEST FILE

The EICAR* Standard Anti-virus Test File is safe to use for test purposes because it is not a virus, and does not include any fragments of viral code. It is a legitimate DOS program that consists entirely of printable ASCII characters. The file lets you simulate safely what happens when Sophos Anti-Virus detects malicious code. When you attempt to run the file, it will be “detected” as though it were a real virus and (customizable) alert messages will be generated.

Using the EICAR file, you can also see the various kinds of report that can be generated.

You can download a copy of the test file at www.eicar.org

Note

Because the EICAR file is not a real virus, it cannot be cleaned by Sophos Anti-Virus and you will need to delete the file manually

APPENDIX III

OTHER SOPHOS PRODUCTS AND SERVICES

Sophos Security and Data Protection

Sophos Email Security and Data Protection

Sophos Email Security and Control is a choice of software solutions and fully integrated Email Appliances, providing effective and intelligent protection against viruses, spyware, Trojans, spam, offensive content and data loss.

Sophos Web Security and Control

Sophos Web Security and Control includes the software required and a fully integrated Web Appliance to protect against the full range of web threats, providing a complete infrastructure for secure browsing and eliminating the complexity of administering effective web security.

Sophos NAC Advanced

Sophos NAC Advanced is a software-based solution that gives you the ability to control who and what is connecting to your network. Sophos NAC Advanced is for organizations that want more sophisticated policy control than the NAC functionality delivered through Endpoint Security and Data Protection.

Sophos SafeGuard Enterprise

SafeGuard Enterprise is a modular data protection control solution that enforces policy-based security for PCs and mobile devices across mixed environments. It is fully transparent to end users and is easy to administer from a single central console. SafeGuard Enterprise provides multi-layered endpoint data security by combining encryption and data leakage prevention (DLP).

SAV Interface

SAV Interface™ enables software vendors, OEMs, ISPs and ASPs to integrate Sophos malware detection into their own industry-standard firewalls, gateways, and similar solutions.

Sophos small business solutions

Sophos small business solutions provide award-winning virus, spyware, and spam protection to enterprises with little or no IT expertise.

Sophos Alert Services

Sophos ZombieAlert™ Service provides you with immediate warning if spammers have hijacked any of your organization's computers to send spam or launch denial-of-service attacks.

www.sophos.com/products/enterprise/alert-services/zombiealert.html

Sophos PhishAlert™ Service provides fast, near real-time alerts of phishing campaigns, so that you can take steps to shut down an imitation website and protect your organization's customers.

www.sophos.com/products/enterprise/alert-services/phishalert.html

Sophos WebAlert™ Service delivers an early warning if any web pages in your domain have been hacked or are hosting malware.

www.sophos.com/products/enterprise/alert-services/webalert.html

Sophos Global Support Services

Support is not just about providing updates or helping with installations. It is about sharing our expertise to give you the very best protection.

Our in-house team of experts is trained in both Sophos solutions and third-party technologies.

Whenever you contact Sophos Global Support Services you will be speaking to a fully trained Sophos employee – not a call taker based in an overseas call center.

Technical support

A global team of Sophos experts provides 24-hour help year round with installing, configuring and upgrading our products, and resolving any technical issues.

Standard Support is available around the clock, every day of the year and is included at no extra cost in all subscription licences. For perpetual licences, Standard Support must be purchased separately. Premium and Platinum Support are available for an additional fee, based on your license cost, and provide penalty-backed service level agreements.

Professional Services

Sophos Professional Services provides the skills to implement and maintain your security solutions. We have a range of standard and customized services to give you all the help you need. Our services can be delivered on site or remotely, and ensure the maximum return on your organization's investment in Sophos.

Technical training

Sophos Technical Training runs courses and workshops around the world to help organizations deal with increasingly complex and evolving threats. Courses cover endpoint, email and web security and our customized packages can meet your specific requirements.

For more details, visit www.sophos.com/support/services

Free tools

Sophos provides a number of tools can be used to reduce vulnerabilities and threats. They are free downloads that utilize our most up-to-date technologies and information.

Sophos Computer Security Scan

http://www.sophos.com/products/free-tools/sophos-computer-security-scan.html

Use our free Sophos Computer Security Scan to see the threats your company's security software missed. Detect malware, unwanted devices and applications that can cause data loss, like removable media or peer-to-peer software, games and more.

Endpoint Assessment Test

www.sophos.com/products/free-tools/sophos-endpoint-assessment-test/

Use our free Endpoint Assessment Test to assess your security. Scan a computer to find out if any OS patches are missing, and whether all security applications are up to date and active.

Application Discovery Tool

www.sophos.com/products/enterprise/applicationdiscovery/eval

Use our free Application Discovery Tool to identify and locate unauthorized applications on your network that Sophos can control. The tool will operate alongside your existing anti-virus software.

Sophos Threat Detection Test

http://www.sophos.com/products/free-tools/sophos-threat-detection-test.html

Use our free Threat Detection Test to check your existing anti-virus protection. This tool will scan and find any viruses, spyware, adware or zero-day threats that might have by-passed your existing protection. The test can be run without uninstalling or deactivating your current anti-virus software

Sophos Anti-Rootkit

http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html

Use our free Sophos Anti-Rootkit software to eliminate rootkits. This tool scans, detects and removes any rootkit that is hidden on your computer using advanced rootkit detection technology.

For more information on free tools visit
http://www.sophos.com/products/free-tools/

SOPHOS

Boston, USA | Oxford, UK

© Copyright 2009. Sophos. All rights reserved. All trademarks are the property of their respective owners.

rg/091215